CVP Smart License CSSM 인증서 가져오기 절차

목차

문제

CVP 통화 서버에서 SmartAgent 로그에서 스마트 라이센싱 "서명 확인" 오류가 발생했습니다. 정상적인 라이센싱 상태 업데이트 프로세스 중에 서명 확인 오류를 해결하려면 CSSM(Cisco Smart Software Manager) 인증서를 CVP 키 저장소로 가져와야 합니다. 적절한 CSSM 인증서 체인이 없으면 CVP는 Cisco Smart Software Manager와의 라이센스 거래를 검증할 수 없으므로 라이센스 규정 준수 문제가 발생합니다.

환경

- Cisco CVP(Customer Voice Portal) Call Server 버전 12.6.2
- Contact Center Software - PCCE(Packaged Contact Center Enterprise)
- CVP 서비스: 호출 서버, WSM(웹 서비스 관리자), VXML 서버
- 인증서 관리를 위한 Java JCEKS 키 저장소 형식
- CSSM(Cisco Smart Software Manager)과 Smart Licensing 통합

해결

CSSM 인증서를 CVP 통화 서버 키 저장소로 가져오려면 다음 세부 단계를 수행합니다.

1단계: 키 저장소 비밀번호 식별

관리자로 명령 창을 열고 CVP 홈 디렉토리로 이동하여 키 저장소 비밀번호를 해독합니다.

```
cd %CVP_HOME%\bin
DecryptKeystoreUtil.bat
```

모든 후속 keytool 명령에 필요한 대로 이 유틸리티에 표시된 비밀번호를 기록합니다.

2단계: 현재 키 저장소 백업

보안 디렉터리에서 기존 키 저장소의 백업을 만듭니다.

```
cd %CVP_HOME%\conf\security
copy .keystore backup.keystore
```

3단계: 현재 키 저장소 내용 내보내기

참조를 위해 키 저장소에 있는 모든 현재 인증서 목록을 생성합니다.

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp.tx
```

생성된 파일을 검토하여 현재 인증서 인벤토리를 파악합니다.

4단계: CSSM 인증서 다운로드

CVP Licensing 페이지의 Transport URL에서 필요한 CSSM 인증서 체인을 가져옵니다. 인증서 요구 사항은 인증서 유형에 따라 다릅니다.

CA 서명 인증서의 경우: 루트 및 중간 인증서를 개별적으로 .cer 형식으로 다운로드합니다.

자체 서명 인증서의 경우: CSSM 인증서를 직접 다운로드합니다

인증서 파일을 CVP 보안 디렉토리에 저장합니다.

```
%CVP_HOME%\conf\security
```

5단계: CSSM 루트 인증서 가져오기(CA 서명)

CA 서명 인증서의 경우 루트 인증서를 먼저 가져옵니다.

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

6단계: CSSM 중간 인증서 가져오기(CA 서명)

중간 인증서가 있는 경우 다음 명령을 사용하여 가져옵니다.

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

7단계: 자체 서명 CSSM 인증서 가져오기(대체)

자체 서명 인증서의 경우 CSSM 인증서를 직접 가져옵니다.

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

8단계: 인증서 가져오기 확인

키 저장소에 새 인증서가 있는지 확인합니다.

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp_ne
```

새 인증서 목록을 검토하여 CSSM 인증서를 성공적으로 가져왔는지 확인합니다.

9단계: 재부팅 및 서비스 확인

CVP 서버를 재부팅하고 재시작 시간을 기록합니다. 재부팅 후 모든 CVP 서비스가 시작되었는지 확인합니다.

- 호출 서버
- WSM(웹 서비스 관리자)
- VXML 서버

서비스 시작 후 약 20분 정도 기다렸다가 검증을 진행합니다.

10단계: 확인 검증

다음 검증 단계를 수행합니다.

SmartAgent 로그 확인:

C:\Cisco\CVP\logs\WSM으로 이동하여 Date Modified(수정 날짜)별로 정렬합니다. SmartAgent 로그에서 가장 최근 15분 상태 보고서를 검토합니다. 확인 서명 예외는 다시 시작 시간 후에 더 이상 나타나지 않아야 합니다.

라이센싱 상태 확인:

CVP 라이센싱 페이지에 액세스하여 시스템에서 오류 없이 "등록됨" 및 "규정 준수 중" 상태를 표시하는지 확인합니다.

롤백 절차(문제 발생 시)

인증서 가져오기 프로세스 중에 문제가 발생하면 다음 롤백 단계를 수행합니다.

1단계: 모든 CVP 서비스 중지(통화 서버, WSM, VXML)

2단계: 보안 디렉토리로 이동합니다.

```
cd %CVP_HOME%\conf\security
```

3단계: 수정된 키 저장소를 삭제합니다.

```
del .keystore
```

4단계: 백업 키 저장소를 복원합니다.

```
rename backup.keystore .keystore
```

5단계: 모든 CVP 서비스 다시 시작

원인

CVP 통화 서버 키 저장소에는 Cisco Smart Software Manager의 디지털 서명을 검증하는 데 필요한 CSSM 인증서 체인이 포함되어 있지 않습니다. 스마트 라이센싱 작업 중에 CVP는 인증서 기반 서명 검증을 사용하여 라이센싱 통신의 신뢰성을 확인합니다. Java JCEKS 키 저장소에 적절한 CSSM 인증서가 없으면 이러한 서명 확인 시도가 실패하여 라이센스 트랜잭션 오류 및 잠재적 규정 준수 문제가 발생합니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.